Downloaded from orbit.dtu.dk on: May 05, 2023

DTU Library

Extending supply chain risk and resilience frameworks to manage cyber risk

Sepúlveda Estay, Daniel Alberto; Khan, Omera

Publication date:
2015

Document Version
Publisher's PDF, also known as Version of record

Link back to DTU Orbit

Citation (APA):
Sepúlveda Estay, D. A., & Khan, O. (2015). *Extending supply chain risk and resilience frameworks to manage cyber risk*. Paper presented at 22nd EurOMA Conference, Neuchâtel, Switzerland.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Extending supply chain risk and resilience frameworks to manage cyber risk

Daniel Alberto Sepulveda Estay (dasep@dtu.dk)
Technical University of Denmark - DTU

Omera Khan
Technical University of Denmark - DTU

Abstract

This paper proposes two complementary tools for the description and quantification of dynamic effects arising from supply chain cyber-attacks. The first tool proposes a comprehensive analysis of the problem space through system dynamics methods, to identify explicitly mental models regarding aspects such as stakeholders, relevant relationships, feedback effects and potential policy levers. The second tool is proposed as a way of transitioning towards a dynamic analysis of the problem of cyber-attacks on supply chains, and is complementary to existing risk analysis tools.

Keywords: Supply chain, cyber-risk, resilience

Introduction

Cyber-risks are an increasingly relevant phenomenon in supply chain management enabled by an information technology-dependent, and increasingly complex supply network with ubiquitous access to technology. This is evidenced by recent cyber-attacks on organizations, targeting anywhere from their financial systems to confidential product or customer information, with potentially severe effects to reputational capital, supply operations, and production processes, to name a few. A key difficulty with cyber-attacks is that often companies will not know that they are at risk until they are being attacked.

Competitive pressures are forcing companies to be responsive, and to consider network competition where "prizes will go to those organizations that can better structure, co-ordinate and manage the relationships with their partners in a network committed to delivering superior value in the final market place" (Christopher, 2011). Supply chains are thus IT-dependent complex networks of agents in constant exchange of information, i.e., data, products and financial resources.

The two aspects crucial to executives when looking to reduce vulnerabilities are security- a preventive aspect which leads to the reduction of the likelihood of a disruption; and resilience- the organizational capabilities for returning to normal operating conditions after a disruption (Sheffi, 2005). Since cyber-attacks can potentially access and impact every company in a shared network, this system will only be as resilient as the weakest link in the supply network.

Traditional risk management theory has been based on a process of risk identification (modes of failure), risk impact evaluation, risk prioritization, preventive action toward diminishing the probability of occurrence for the risks with a priority above a certain threshold, and subsequent control that these preventive actions were executed.

However, increasing supply chain complexity is creating modes of failure in a supply chain beyond the preventive analysis capabilities of the organization. Therefore, it is becoming increasingly difficult to foresee every possible way in which a supply chain can be disrupted.

In the case of cyber-risks, this is particularly relevant, as increased dependence on IT has been reported to result in an increased number of suppliers in a network (Dederick et al., 2008) hence increasing the number of links where cyber-attacks can root and deploy to other parts of the target network.

There seems to be a consensus on what constitutes supply chain risk management (Khan et al., 2007), and considers the identification, analysis and control of those supply chain risks that could financially undermine the assets or earning capability of an organization, within the context of its overall aims. Methods have been developed to manage uncertainty in the supply chain, through coordination procedures (Sales & Operations Planning, Collaborative Planning Forecasting & Replenishment) for existing operations, and risk management (e.g., Business Continuity Planning) to detect additional procedures/capabilities required to better manage disruption events.

This work analyses the literature on supply chain resilience frameworks and cyber-attack types to analyse the application of these frameworks to cyber risks. This work then proposes two types of tools as contributions to bridging the research gap. One of the tools is intended towards a systemic description of the problem landscape for creating a research agenda, and as a tool to explicitly map the mental models (Doyle et al., 1998) of the problem at hand when used through group model building, for example. The second tool seeks to bridge the gap between current accepted practices, which themselves fall short for the adequate description and management of a dynamic problem, and which is presented as a complement to existing risk assessment tools.

Cyber-attack types

Our analysis of the literature showed that the types of cyber-attacks that can affect supply chains have been gathered from two main sources: a) the theoretical development of cyber-attack taxonomies and classifications based in information technology research (deductive method), and b) through the record and classification of attacks derived from information gathered with industrial practitioners (inductive method).

Furthermore, the analysis showed relevant contributions through the deductive approach of the description of supply chain cyber risks from the point of view of IT vulnerabilities. These categorizations are derived from a systematic assessment of IT/SC structure, are later tested against case studies, and are normally presented as peer-reviewed articles.

Gordon (Gordon et al., 2006) developed a cybercrime categorization for these events by combining a technology and a human component. If the cyber-attack contained mainly technological components, it was denominated type 1, and type 2 if the components were mainly human in nature. They further characterized type 1 events as singular or discrete from the perspective of the victim, facilitated by the use of crime-ware software and that the introduction of this software may not necessarily be facilitated by vulnerabilities. On the other hand, they characterized type 2 events as facilitated by processes that do not fit

under crime-ware (e.g., Instant Messaging, FTP file transfer), and as having in general repeated contacts or events from the perspective of the user.

Simmons et al., (2014) developed a cyber-attack taxonomy derived from computer program security flaws, which classifies threats according to potential defences, and thus facilitating the proposal of strategies to manage these risks. Through the identification of the ways in which attacks could take place, this group proposes a series of "vectors" which form the evaluation framework AVOIDIT (Attack Vector, Operational Impact, Defence, Information Impact, and Target). This framework uses a tree structure to categorize and enumerate the ways in which an attack might occur.

On the other hand, an inductive approach has been followed by organizations who monitor cyber-attack events to industrial organizations. These studies are normally presented as non-peer-reviewed articles or reports. This approach is inductive since it starts form the observable experience of cyber-attacks to industry, to subsequently propose a categorization or taxonomy that might be more generalizable. The incentives for private organizations to generate these reports is to evidence themselves as subject-matter-experts when offering cyber-security consulting services to industrial companies. Additionally, several multinational organizations have started regular updates on cyber security with information from its members, such as the Organization of American States (OAS, 2013), or the World Economic Forum (WEF, 2008).

Verizon (Verizon, 2014) has developed Data Breach Investigation Reports (DBIR), published yearly, and which gathers information about information breaches from 50 contributing organizations and spanning 95 countries around the world. This report identified 9 main types of breaches, i.e., cyber- espionage, DOS Attacks (denial of service), crime ware, web app attacks, insider misuse, miscellaneous errors, physical theft and loss, and payment card skimmers. These attack patterns described 92% of the 100.000 incident database taken into consideration by this study.

The OAS is issuing a yearly report that shows a 12-40% increase in reported cyber-attack incidents yet indicates in their latest report, "most states do not differentiate between the types or severity of cyber incidents they reported", and that "divergent views show that more specific data is needed to accurately diagnose the threat" (OAS, 2013).

The World Economic Forum (WEF, 2015) identified cyber risks as a high-impact technological risk and ranked it as above average both in likelihood and impact with respect to other types of risks. The WEF also makes a distinction between state-sponsored, state-affiliated, criminal, and terrorist cyber-attack types.

Supply chain resilience frameworks

The earliest reference to supply chain resilience frameworks found in our literature research corresponds to the frameworks proposed by Christopher & Peck at Cranfield University (Christopher el at, 2004), and the framework proposed by Sheffi & Rice at MIT (Sheffi et al., 2005). These approaches were largely complementary, both descriptive in nature and with some points in common such as the requirement for a risk culture in the organization as well as the explicit indication of a necessary trade-off between redundancy and efficiency at the time or developing organizational resiliency. However, while Christopher talks about capabilities required for resilience building and critical path identification, Sheffi concentrates on the analysis and mapping of vulnerabilities, and describes the dynamic behaviour of the performance of a supply chain through a disruption, proposing the concept of "disruption profile", with the qualitative identification of eight main phases within this disruption profile. Additionally,

Christopher emphasizes on "agility" for the deployment of existing resources (resulting from velocity and visibility within the organization) as a requirement for resilience, while Sheffi talks about "flexibility" and the transitory, alternate use of existing resources.

Subsequent models build on these initial frameworks, and are characterized by approximations to the empirical quantification of resilience through case studies. Blackhurst (Blackhurst et al., 2011) and her team in 2011, identified thirteen resilience enhancers and seven resilience reducers in the organization. On the other hand, Pettit & Fiskel (Pettit et al., 2010) from Ohio State University, proposed a SCRAM framework (supply chain resiliency assessment and management) in 2010. Through case studies, Pettit identifies seven "vulnerability factors" and fourteen "capability factors". Additionally, Pettit identifies an existing trade-off between developing too many unused capabilities through excessive investment, which would erode profits, versus developing too many vulnerability factors through insufficient investment, which would also erode profits through insufficient response to disruptions.

Work by Linkov (Linkov et al, 2013) at Arizona State University together with the US Army in 2013, proposes the concept of cyclic disruption event management through which an organization will need to prepare, absorb, recover from and adapt to disruptions, point at which a new cycle begins.

A summary of the chronology and relationship between these frameworks is presented in Figure 1:

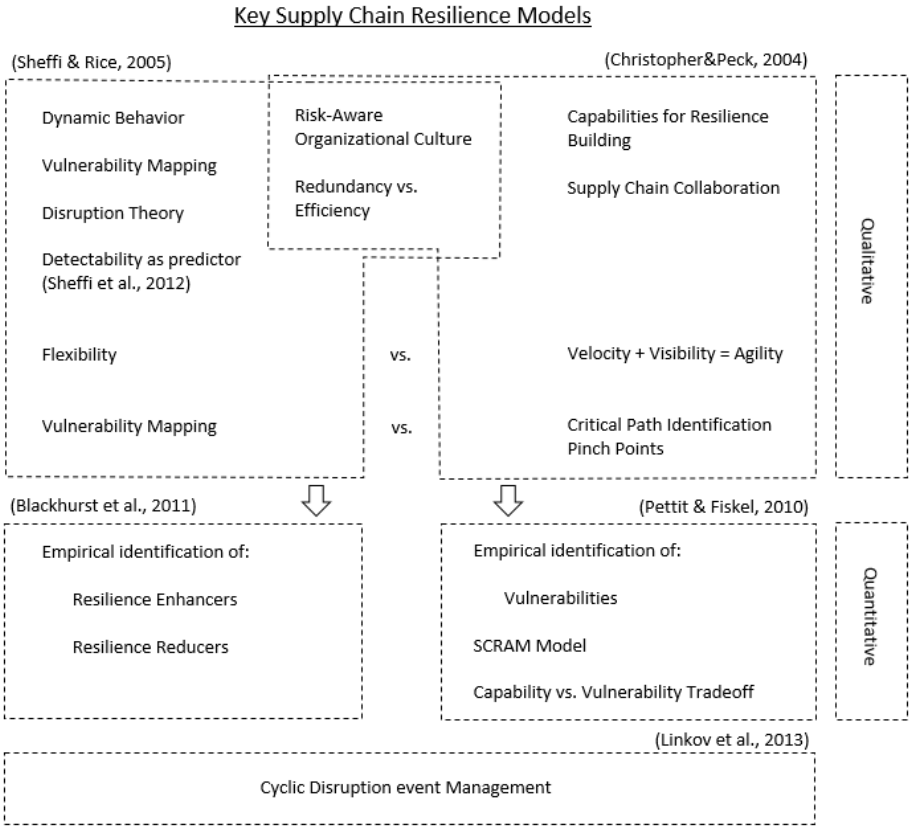

Figure 1 Key supply chain resilience models

In a recent 2014 article, Simchi-Levi at MIT described a technique for assessing the effect of disruptions on a supply network through the use of Time to Response - TTR, Performance Impact scores – PI, and a Risk Exposure Index – REI (Simchi-Levi et al., 2014). This method simulates the disruption response of a system by removing one node in the supply system at a time during the TTR, and optimizing system response, thus obtaining a PI for each node. The node with the largest PI is assigned a REI of 1,0, and the other nodes are assigned a REI relative to this Larges Rei value. These authors claim this method to better guide investment in areas with the greatest impact, is based on numerical optimization, and as a simulation it allows for experimentation with different TTR values.

Literature has documented the limitations of current risk assessment methods (Khan et al., 2007). These introduce assessment team biases, have a strong influence of past subjective experiences, are largely linear and static analyses, and deliver little information towards managing exposure to new or extreme events. Additionally, the assessments results can show a misalignment with management processes, hindering or delaying the implementation of assessment recommendations (Osha, 2008).

If the risk assessment of potential events is based on the experience of the team making the assessment, it is expected that the results will always run behind the new emergent modes of attack, characteristic of the cyber threats.

Discussion: Gap identification and tool proposals

Our literature research appears to show some initial proposals for a research agenda in the area of supply chain resilience in general (Khan & Zsidisin, 2011), and cyber resilience in particular (Khan & Sepulveda, 2015). We propose that this, as yet, limited literature on the topic is founded both in 1) a lack of evidence of a systemic perspective of the problem landscape to define a coherent problem space and thus guide research efforts, and 2) the lack of proposed complementary tools to established supply chain risk assessment methods, which may introduce ways of quantifying the dynamic response of a supply chain to disruptions starting from a familiar paradigm to practitioners.

As potential contributions to bridging the gap, this paper will argue for the use of a systemic analysis of the problem landscape description, as well as for the use of detectability for quantifying the dynamic response of systems by adding this parameter to existing FMCA (Failure mode and Criticality Analysis) processes.

Tool type 1: Systemic outlook of the problem landscape

Our literature research did not find any systemic analysis of the cyber risk issue, which might illustrate, even in qualitative terms, the relationships between the different agents in the problem, and which might account for both short and long-term impacts. System dynamics tools such as causal loop diagrams (CLD) and stock and flow diagrams (SFD) and can be used to map out and quantify the known relationships that exist between actors within a complex system (Sterman, 2000), and in order to explore and understand the evolution of these relationships and behavioural feedbacks over time. Such a diagram/model will be by definition an approximation to reality, and has to have a correct balance between aggregation and atomization of variables for the problem we are trying to describe.

It is relevant to keep in mind the interaction between the static configuration of a system and its dynamic behaviour. This is shown in Figure 2.

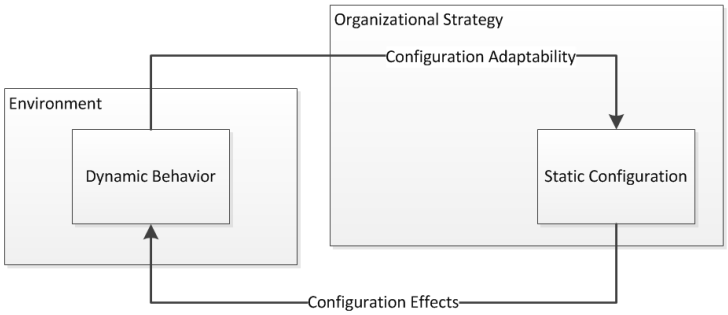

Figure 2 Relation between supply chain dynamic behaviour and static configuration

Figure 2 shows a feedback loop between an organization's supply chain static configuration and the dynamic behaviour of this supply chain when subject to its environment. This dynamic behaviour then feeds back into, and adjusts the static configuration according to the available adaptability skills in the supply chain, in an ongoing, circular process.

Since the resilience of an organization in general, and cyber-resilience in particular is not an event, but a series of connected events which develop in time as a result of an underlying system structure (i.e., behaviour), traditional methods of risk analysis fall short of describing these behaviours correctly, and we argue are ill-equipped to manage these types of problems. This is tantamount to explaining why breaks are necessary or how they should be used in a car, by analysing a series of photos of the car in movement; no amount of photos will correctly convey the effects of the car mass or velocity, for example, in how the breaks should be applied.

A first approximation to a causal loop diagram of the problem of cyber-attacks to supply chains is shown in Figure 3. This diagram shows three main social spaces where this problem develops. The company space reflects the dynamics within an industrial organization that promote or hinder investment in cyber-capabilities, how this investment relates to the vulnerabilities and resulting number of cyber-attacks, and finally the effect this has on customer satisfaction. The hacker space shows the internal process of hacker prestige and hacker legal prosecution which respectively promote and hinder the development of cyber-attack modes and the number of cyber-attacks. It is important to note that these two spaces in this model share at least the number of attacks and the technology available. A third space, the public space is present as it creates the social tension to promote prosecution of hackers due to the lower level of customer satisfaction which results from the hacker attacks.

A next step after a systemic understanding of the problem landscape, but to which no tools have yet been proposed, is to investigate and analyse the dynamics of the system. To this end, an SFD is necessary, which not only quantifies the relationships between actors that were identified in the CLD, but also integrates dynamic effects such as sources of systemic inertia, important delays in the relationships, as well as the identification of policy levers.

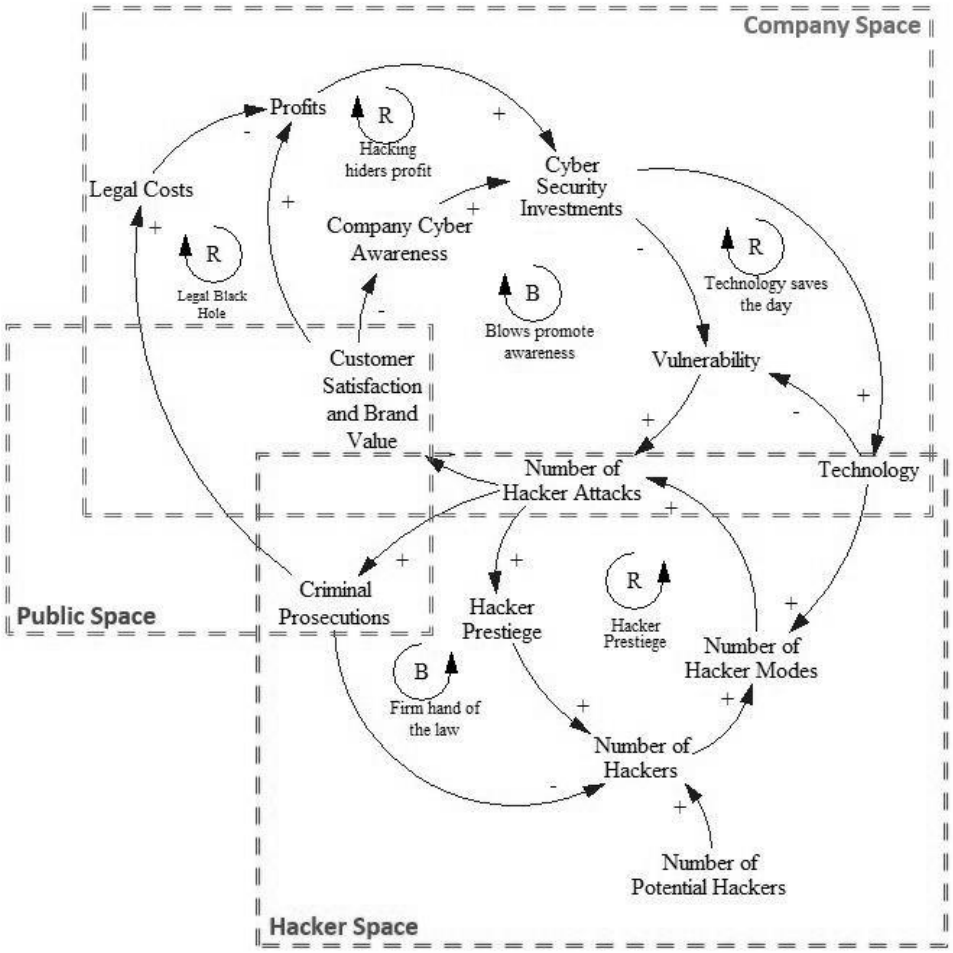

Figure 3 Systemic Analysis if the Problem Landscape

Tool type 2: Bridging the gap- Dynamic response through detectability

Dynamic behaviour is not an easy subject to convey to practitioners. Therefore a second type of tool proposed in this work relates to tools, which might help manage these effects in time, through complements to tools which have practitioner use and acceptance.

Detectability as a risk assessment factor in supply chain risk management had been proposed in the past (Sheffi et al., 2012; Lee, 2007) but has eluded widespread application for risk assessment processes, as detectability is considered by some a damage-containment (event mitigating) parameter, more than a risk mitigation factor (Youssef et al., 2010). Others argue the counter-intuitive nature of the event detectability when used in conjunction with probability and severity: while the higher probability or severity associated with a supply chain risk relate to a disruption event that is more relevant, a higher detectability, corresponds to an event that is in fact less relevant. Therefore, measures of "un-detectability" have rather been suggested.

We argue here that it is a convenient way to reflect the degree of perceived resilience in the organization, and therefore of its dynamic response to disruptions. Based in the disruption model presented by Sheffi & Rice (Sheffi et al., 2004), consider the evolution of a supply chain process KPI through a disruptive event, as illustrated in Figure 4:

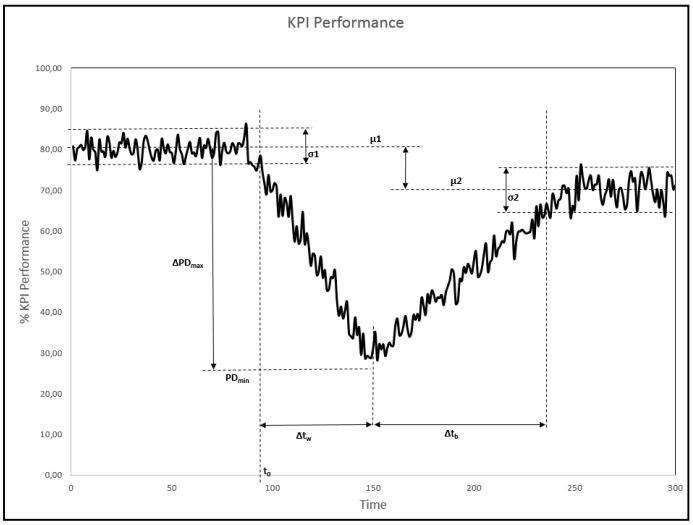

Figure 4 Quantitative description of a disruption event curve

This generic KPI, before the disruptive event had an average value of μ_1 and a standard deviation of σ_1. At time t_0 this supply chain starts to experience a decrease in this KPI beyond the normal levels. This reduction in performance continues to a point when the organization reacts and the performance reverts its downward trend at time $t_0+\Delta t_w$, reaching a new level of stable operation at time $t_0+\Delta t_w+ \Delta t_b$, with a new mean value for this KPI of μ_2 and a standard deviation of σ_2. At this point we make a proposition for the characteristic of this process development:

Proposition 1: The unwanted organizational effects of a disruptive event will have a direct relationship with the total duration of the disruption (Δt_w and Δt_b in Figure 4

Proposition 2: The unwanted organizational effects of a disruptive event will have a direct relationship with the decrease in the performance of the supply chain through the duration of the disruption (ΔPD_{max} in Figure 4)

Now, consider two equivalent processes with different detectability. The effect of this difference when subjected to a disruptive event can be illustrated in Figure 5.

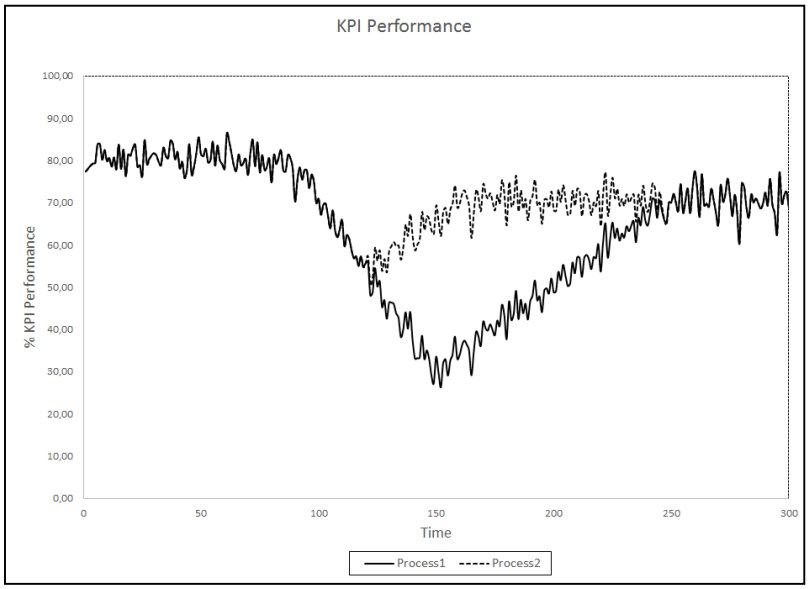

Figure 5 Process comparison

Process 2 as illustrated, has a better detectability (i.e., starts earlier with its KPI performance recovery) and is likely to have a smaller organizational adverse effect than Process 1. Hence, Process 2 could be identified as more resilient than Process 1. This earlier reaction in Process 1 can occur due to any combination of a series of organizational capabilities, among them, "awareness" to identify unusual operating conditions, which trigger disruption mitigation actions, and /or "flexibility", to quickly generate the organizational adaptations for disruption mitigation. These capabilities relate to the "agility" factor for supply chain resilience identified by Christopher (Christopher et al., 2003). Additionally, the way these capabilities interact during a disruption event, and how these capabilities and system structure relate to cyber-attack effects should be analysed through a systemic model.

Such a tool would be especially well suited to supply chains where KPI performance measurement is already taking place frequently or online. The quantity and speed with which cyber-attacks affect supply chains, makes these type of tools especially well suited to these types of risks. The methods for such an implementation stand out as relevant research opportunities derived from this work.

Conclusions

The relevant adverse effects, as well as the increasing number of cyber-attacks on supply chains, together with the limited research that has been undertaken to describe and manage this phenomenon, makes this a very significant area of research.

Additionally, any research that is conducted on cyber risk in the supply chain will necessarily need close interaction with practitioners, in order to keep up with the speed of development of these types of threats, towards shorter cycles of tool development, tool proposal and tool validation. Furthermore, a comprehensive research framework which has identified all relevant actors and stakeholders in the supply chain and problem landscape and has made informed decisions on the priority of cyber resilience development for each supply chain area and system participant, should be developed.

This paper lays out proposals for bridging some relevant gaps, which serve as stepping stones towards tools and methods which might be both accepted and applicable by practitioners, as well as coherent with a systemic understanding of the complex problem of cyber risks and security in the global supply chain.

References

Blackhurst, J., Dunn, K., Craighead, C. (2011), "An empirically derived framework of global supply resiliency", *Journal of Business Logistics*, Vol. 32, No. 4, pp. 374-391.

Christopher, M., Peck, H. (2003), "Supply chain resilience, final report on behalf of the department of transport", *University of Cranfield*.

Christopher, M. (2011), "Logistics and Supply Chain Management", *Financial Times Series*, London, p.213.

Dederick, J., Sean, X., Zhu, K. (2008), "How does information technology shape supply chain structure? Evidence on the number of suppliers", *Journal of Management Information Systems*, Vol. 25, No. 2, pp. 41-72.

Doyle, J.,Ford, D. (1998), "Mental models concepts for system dynamics", *System dynamics review*, Vol. 14, No. 1, pp. 3-29.

Gordon, S., Ford, R. (2006), "On the definition and classification of cybercrime", *Journal of Computational Virology*, Vol.2, pp. 13-20.

Khan, O., Burnes, B. (2007), "Risk and supply chain management: creating a research agenda", *The International Journal of Logistics Management*, Vol. 18, No. 2, pp. 197-216.

Khan, O. Zsidisin, G. (2011), "Handbook for Supply Chain Risk Management: Case Studies, Effective Practices and Emerging Trends", *J. Ross Publishing*

Khan, O., Sepulveda, D.A. (2015), "Supply Chain cyber resilience: crating an agenda for future research", *Technology and Information Management Review*, Vol. 5, No. 4

Lee, W. (2007), "Risk Assessment modelling in aviation safety management", *Journal of Air Transport Management*, Vol. 12, No. 5, pp. 267-273.

Linkov, I. (2013), "Measurable resilience for actionable policy", *Environmental science & technology*, Vol. 47, No. 18, pp. 10108-10110.

OAS. (2013), "Latin American and Caribbean cybersecurity trends and government responses", *http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf*, access 30 April 2015.

Pettit, F., Croxton, K. (2010), "Ensuring supply chain resilience: development of a conceptual framework", *Journal of Business Logistics*, Vol. 31, No. 1, pp. 1-21.

Simchi-Levi, D., Schmidt, W., Wei, Y. (2014), "From superstorms to factory fires: managing unpredictable supply-chain disruptions", *Harvard Business Review*, Vol. 92, No. 1-2, pp. 96.

Sheffi, Y. (2005), "The Resilient Enterprise", *MIT Press Books*, pp. 14.

Sheffi, Y., Vakil, B., Griffin, T. (2012), "Risk and Disruptions: New software tools", *http://sheffi.mit.edu/sites/default/files/Risk_and_Disruptions_V9.pdf*, access 30 April 2015.

Simmons, C. (2014), "AVOIDIT: A cyber-attack taxonomy", *9th annual symposium on information assurance* (Asia '14).

Sterman, J. (2000), "Business Dynamics", *Irwin/McGraw-Hill*, Boston, pp. 1-39.

Tranfield, D., Denyer, D., Smart, P. (2003), "Towards a methodology for developing evidence-informed management knowledge by means of systematic review", *British Journal of Management*, Vol. 14, No. 3, pp. 207-222.

Verizon. (2014), "2014 Data Breach Investigations Report", *http://www.verizonenterprise.com/DBIR/*, access: 30 April 2015.

WEF. (2008), "Global risks landscape 2015", *http://www3.weforum.org/docs/WEF_Global _Risks_2015_Report15.pdf*, access: 30 April 2015.

Youssef, N., Hyman, W. (2010), "Risk analysis: Beyond probability and severity", *Medical Device and Diagnostic Industry*, Vol. 32, No. 8.